ABSTRACT OF THE DISCLOSURE

An optimized approach for arriving at a shared secret key in a multicast or broadcast group environment is disclosed. The key exchange method is mathematically equivalent to the standard broadcast version of the Diffie-Hellman public-key algorithm. However, from an implementation perspective, nodes within a multicast or broadcast group are treated in a binary fashion, whereby a shared secret key is generated for a pair of nodes at a time. Once the shared secret key is computed by the pair, the nodes within the pair are viewed as a single entity by a node that is to be joined. This process is iteratively performed until all the nodes within the multicast group attain a common shared secret key. Under this approach, the number of messages exchanged between the nodes for establishing the secured channel is significantly reduced compared to the standard broadcast Diffie-Hellman method.